The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

11/12/2013

SUBJECT:

Vulnerability Microsoft ActiveX control could allow for remote code execution (MS13-090)

OVERVIEW:

A vulnerability has been discovered in the InformationCardSigninHelper Class ActiveX control, which could allow for remote code execution. The InformationCardSigninHelper is an add-on that is used by Microsoft CardSpace. CardSpace is a personal identity management platform. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2003 – Non Core Installation
- Windows Server 2008 – Non Core Installation
- Windows Server 2008 R2 – Non Core Installation
- Windows Server 2012 – Non Core Installation
- Windows Server 2012 R2 – Non Core Installation

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in the InformationCardSigninHelper Class of ActiveX, which could allow for remote code execution. The InformationCardSigninHelper Class is a default add-on for Internet Explorer which cannot be disabled. The vulnerability can be exploited when a user views a specially crafted webpage through Internet Explorer. When the user visits the specially crafted webpage, remote code execution can occur.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites, follow links, or open files provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

https://support.microsoft.com/kb/2900986

https://technet.microsoft.com/en-us/security/bulletin/ms13-090

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3918